UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/552,955	10/14/2005	Fredrik Lindholm	P18053-US1	2497

27045 7590 08/03/2009

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
NGUYEN, TRONG H	
ART UNIT	**PAPER NUMBER**
2436	

MAIL DATE	DELIVERY MODE
08/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/552,955	LINDHOLM ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,13-32 and 34-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,13-32 and 34-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 04/03/2009. In response to the office action mailed on 11/03/2008, **claims 1-3, 6, 10, 20, 25-27, 32, 41, 43, and 45** have been amended and **claims 12, 33, 46, and 47** have been canceled. Pending claims include **claims 1-11, 13-32, and 34-45**.

The objection to title of the specification and the abstract has been withdrawn due to Applicants' amendment.

The objection to **claims 1-3**, **10**, **26-27**, **32**, **43**, **and 45** has been withdrawn due to Applicants' amendments.

The rejection of **claims 1, 25, and 41** under 35 USC 112, second paragraph has been withdrawn due to Applicants' amendment.

Examiner Notes

2. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

3. Applicants' arguments filed on 04/03/2009 have been fully considered but the following argument(s) is/are not persuasive.

Applicants argue that:

i. Schutzer does not teach assigning individual (i.e. unique) authentication tokens to the respective units in a group based on a password such that each authentication token is irreversibly determined by the password.

In response to applicant's arguments:

i. The Examiner respectfully disagrees. Although, Schutzer was originally relied upon to show assigning individual authentication tokens to respective units in a group, Schutzer also discloses assigning individual (i.e. unique) authentication tokens to the respective units in a group based on a password such that each authentication token is irreversibly determined by the password on pars. 0010 or 0024-0025, "An important aspect of the registration process is the **providing of an authenticating token to the user** by the authenticating authority in connection with the user registration. **The authenticating token consists, for example, of a one-way hash (or an index derived from the one-way hash) of user identification information** known only to the authenticating authority and the user, **such as the biometric information and/or shared secret information** and is produced using, for example, a Secure Hash Algorithm (SHA) or a message digest algorithm (MD-5)."

Claim Objections

4. **Claims 1-2, 6, 13, 17-18, 25-26, 30, 34-36, and 41-42** are objected to because of the following informalities:

"said first device" on second to last line of **claim 1** lacks antecedent basis.

"the authentication procedure" on line 3 of **claim 2** lacks antecedent basis.

"the group" on line 2 of **claim 6** lacks antecedent basis.

"the input parameters" on line 2 of **claim 13** lacks antecedent basis.

"the number" on line 2 of **claims 16 and 17** lacks antecedent basis.

"the result" on line 2 of **claim 18** lacks antecedent basis.

"the token secret" on line 12 and last line of **claim 25** lacks antecedent basis.

"the authentication procedure" on line 3 of **claim 26** lacks antecedent basis.

"the group" on line 2 of **claim 30** lacks antecedent basis.

"the input parameters" on line 2 of **claim 34** lacks antecedent basis.

"the number" on line 2 of **claims 35 and 36** lacks antecedent basis.

"the token secret" on line 12 and last line of **claim 41** lacks antecedent basis.

"the authentication procedure" on line 2 of **claim 42** lacks antecedent basis.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 25, and 41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 25 and 41 recite "determining...a token secret using the authentication token of the first unit and the password". However, it is unclear how this "determining" step is being done i.e. deriving, accessing from storage, or… In addition, "creating…the check token…based on the token secret and the password" is also unclear since by "creating", does it mean encrypting, concatenating, or...

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1, 10-11, 13-15, 18, 21, 25, 32, 34, 37, 39, 41, and 45** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard et al. US 7,363,494 (hereinafter "Brainard") in view of Schutzer US 2002/0053035 (hereinafter "Schutzer") and further in view of Kaufman et al. US 5,491,752 (hereinafter "Kaufman").

Regarding claim 1, Brainard discloses "**A method for password-based authentication in a communication system**" as [computer based methods for time-based and password-based authentication (Col. 2, lines 24-25 and line 31)] "**including a group of at least two units associated with a common password,**" as [user 110

and authentication device 120 (corresponding to user 410 and authentication device 420 in Fig. 3) (first unit) and verification computer 150 and computer 140 (corresponding to verification computer 450 and computer 440 in Fig. 3) (second unit) share a secret PIN or password (Fig. 1, Col. 10, lines 50-52 and Col. 5, line 17). Therefore, user 410 and authentication device 420 (first unit) and verification computer 450 and computer 440 (second unit) share a secret PIN or password] "**based on the password such that each authentication token is irreversibly determined by the password**;" as [the PIN (P) can be mapped to another value with a one-way (irreversible) function before being provided as an input to the combination function to generate an authentication code (Col. 10, lines 58-61)] "**determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit** as [authentication code 490A for computer 440 and verification computer 450 (second unit) is generated based on the password or PIN (P1) at authentication device 420 (first unit) (Fig. 3)] "**wherein the step of determining the check token comprises the steps of: creating, at the first unit, the check token for the second unit based on the token secret and the password;**" as [Brainard discloses authentication code 490A is created at authentication device 420 based on the stored secret and the password (Brainard, Fig. 3) and is transmitted to computer 440 (Brainard, Col. 15, lines 28-29)] "**sending the check token to the second unit; and comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, wherein said user of said first device is authenticated if said check token is the same as said authentication**

token of said second unit" as [authentication code 490A is transmitted to computer 440 and verification computer 450 (second unit) and is compared with authentication code 490B. If they are the same, then the user is authenticated (Fig. 3, Col. 15, lines 28-29 and Col. 16, lines 9-12)]

Although Brainard discloses generating authentication tokens based on the password such that each authentication token is irreversibly determined by the password, Brainard does not specifically disclose **assigning individual authentication tokens to the respective units in the group.** Although Brainard discloses determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit, Brainard does not specifically disclose **determining, at a first unit, a check token for a second unit based on the authentication token of the first unit.** In addition, Brainard does not specifically disclose **determining, at a first unit, a token secret using the authentication token of the first unit and the password.**

However, Schutzer discloses assigning individual authentication tokens to respective units in a group based on a password such that each authentication token is irreversibly determined by the password (Par. 0010, lines 8-9 and pars. 0010 or 0024-0025).

Schutzer and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Brainard's authentication method by assigning individual

authentication tokens to respective units in the group as described by Schutzer since it would provide for the purpose of strong but convenient authentication (Schutzer, Col. 1, Par. 0002, line 3).

Furthermore, Kaufman discloses determining, at a first unit (i.e. workstation), a check token (i.e. transmission code) for a second unit (i.e. server) based on an authentication token (i.e. token) of the first unit (col. 9, lines 41-44 and col. 10, lines 18-20). In addition, Kaufman discloses determining, at a first unit (i.e. workstation), a token secret (i.e. password | token or hash (password | token)) using the authentication token of the first unit (i.e. token) and the password (i.e. password) in generating the check token (col. 9, line 62 - col. 10, line 5).

Kaufman, Schutzer, and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer by including determining, at a first unit, a check token for a second unit based on the authentication token of the first unit and determining, at a first unit, a token secret using the authentication token of the first unit and the password as described by Kaufman for the purpose of obtaining an improved method by which a user or other principal in a computing system may authentication to a computer system (Kaufman, col. 1, lines 13-19).

Regarding claim 10, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1, wherein the assigning step further comprises the steps of: determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password**;" as [a stored secret (K) which is non-correlated with the password or PIN (P) is determined at authentication device 120 (corresponding to authentication device 420 shown in Fig. 3) (Brainard, Col. 8, lines 51-53). Therefore, a stored secret (K) is also determined at authentication device 420. Furthermore, this stored secret (K) is accessible to both the authentication device 120 and the verification computer 150 (corresponding to verification computer 450 shown in Fig. 3) (Brainard, Col. 8, lines 60-63). Hence, the stored secret (K) is accessible to both the authentication device 420 (first unit) and verification computer 450 (second unit)] "**and creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password**" as [Schutzer discloses an authentication code being assigned to a user (Schutzer, Col. 1, Par. 0010, lines 9-10). Brainard discloses authentication code 490A being created at authentication device 420 based on the stored secret (K) and the password (P) (Brainard, Fig. 3). Therefore, it is obvious to create an authentication code at authentication device 420 for another device based on the stored secret (K) and the password (P) as described by Schutzer and Brainard if desired].

Regarding claim 11, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 10, wherein the step of determining the**

token secret involves generating the token secret, as a part of an initial set-up procedure" as [Brainard discloses stored secret (K) being determined at manufacturing time or generated and stored in a secure data store initially (Brainard, Col. 8, lines 50-53 and 58-59). Furthermore, Schutzer also discloses shared secret being determined at initial registration (Schutzer, Col. 2, Par. 0024, lines 10-13)].

Regarding claim 13, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 10, wherein the creating step involves using a bijective locking function, the input parameters of which include the token secret and a one-way function of the password**" as [Brianard discloses that an authentication code may be generated by encrypting the hash value of the password and/or other additional values using the stored secret (K) (Brainard, Col. 10, lines 58-61, Col. 14, lines 65-67, and Col. 15, lines 1-2)].

Regarding claim 14, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 13, wherein the locking function is a symmetric encryption function**" as [Brainard discloses the use of symmetric key encryption in verifying authentication code (Brainard, Col. 7, line 65). Hence, Brianard makes it obvious that symmetric key encryption is used in generating authentication code].

Regarding claim 15, Brianard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 13, wherein the locking function is implemented through password-based secret sharing**" as [Brainard discloses the encryption function may take in the hash value of the password (P) and the stored secret (K) and both are shared among the devices as inputs (Brainard, Col. 8, lines 60-62, Col. 10, lines 58-61, Col. 14, lines 65-67, and Col. 15, lines 1-2)].

Regarding claim 18, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1, further comprising the step of sending an authentication response message from the second unit indicating the result of the comparing step**" as [Brainard discloses a message may be communicated to the user 410 (first unit) from computer 440 (second unit) to indicate whether the authentication was successful (Brainard, Fig. 3, Col. 16, lines 24-26)].

Regarding claim 21, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1, wherein critical operations for which authentication is needed are listed in policies in at least one of the units"** as [By disclosing critical operations such as paying funds, moving money and the like require a user to authenticate himself or herself (Schutzer, Col. 4, Par. 0032, lines 1-3), Schutzer makes it obvious that critical operations which require user authentication are listed in policies of the financial institution's system. Therefore, it is obvious to list critical operations which need user authentication in policies of at least one of the devices if desired].

Regarding claim 25, Brainard discloses "**A communication system**" as [computer based system for time-based and password-based authentication (Col. 2, lines 24-25 and line 31)] "**including a group of at least two units associated with a common password, and means for password-based authentication, comprising**:" as [user 110 and authentication device 120 (corresponding to user 410 and

authentication device 420 in Fig. 3) (first unit) and verification computer 150 and computer 140 (corresponding to verification computer 450 and computer 440 in Fig. 3) (second unit) share a secret PIN or password (Fig. 1, Col. 10, lines 50-52 and Col. 5, line 17). Therefore, user 410 and authentication device 420 (first unit) and verification computer 450 and computer 440 (second unit) share a secret PIN or password] "**based on the password such that each authentication token is irreversibly determined by the password**;" as [the PIN (P) can be mapped to another value with a one-way (irreversible) function before being provided as an input to the combination function to generate an authentication code (Col. 10, lines 58-61)] "**means for determining, at a first unit, a check token for a second unit based on the password**" as [authentication code 490A for computer 440 and verification computer 450 (second unit) is generated based on the password or PIN (P1) at authentication device 420 (first unit) (Fig. 3)] "**and means for comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit;**" as [authentication code 490A is transmitted to computer 440 and verification computer 450 (second unit) and is compared with authentication code 490B (Fig. 3, Col. 15, lines 28-29 and Col. 16, lines 9-10)] "**wherein the means for determining the check token further comprises: means for creating, at the first unit, the check token for the second unit based on the token secret and the password**" as [Brainard discloses authentication code 490A is created at authentication device 420 based on the stored secret and the password (Brainard, Fig. 3) and is transmitted to computer 440 (Brainard, Col. 15, lines 28-29)].

Although Brainard discloses generating authentication tokens based on the password such that each authentication token is irreversibly determined by the password, Brainard does not specifically disclose **means for assigning individual authentication tokens to the respective units in the group.** Although Brainard discloses means for determining, at a first unit, a check token for a second unit based on the password, Brainard does not specifically disclose **means for determining, at a first unit, a check token for a second unit based on the authentication token of the first unit.** In addition, Brainard does not specifically disclose **means for retrieving, at the first unit, the token secret using the authentication token of the first unit and the password.**

However, Schutzer discloses assigning individual authentication tokens to respective units in a group based on a password such that each authentication token is irreversibly determined by the password (Par. 0010, lines 8-9 and pars. 0010 or 0024-0025).

Schutzer and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Brainard's authentication method by means for assigning individual authentication tokens to respective units in the group as described by Schutzer since it would provide for the purpose of strong but convenient authentication (Schutzer, Col. 1, Par. 0002, line 3).

Furthermore, Kaufman discloses determining, at a first unit (i.e. workstation), a check token (i.e. transmission code) for a second unit (i.e. server) based on an authentication token (i.e. token) of the first unit (col. 9, lines 41-44 and col. 10, lines 18-20). In addition, Kaufman discloses determining, at a first unit (i.e. workstation), a token secret (i.e. password | token or hash (password | token)) using the authentication token of the first unit (i.e. token) and the password (i.e. password) in generating the check token (col. 9, line 62 - col. 10, line 5).

Kaufman, Schutzer, and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer by including means for determining, at a first unit, a check token for a second unit based on the authentication token of the first unit and means for retrieving, at the first unit, the token secret using the authentication token of the first unit and the password as described by Kaufman for the purpose of obtaining an improved method by which a user or other principal in a computing system may authentication to a computer system (Kaufman, col. 1, lines 13-19).

Regarding claim 32, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25, wherein the means for assigning further comprises: means for determining, at an assigning unit in the group, a token secret common for the group and non-correlated with the password**;" as [a

stored secret (K) which is non-correlated with the password or PIN (P) is determined at authentication device 120 (corresponding to authentication device 420 shown in Fig. 3) (Brainard, Col. 8, lines 51-53). Therefore, a stored secret (K) is also determined at authentication device 420. Furthermore, this stored secret (K) is accessible to both the authentication device 120 and the verification computer 150 (corresponding to verification computer 450 shown in Fig. 3) (Brainard, Col. 8, lines 60-63). Hence, the stored secret (K) is accessible to both the authentication device 420 (first unit) and verification computer 450 (second unit)] "**and means for creating, at the assigning unit, the authentication token for another unit in the group based on the token secret and the password**" as [Schutzer discloses an authentication code being assigned to a user (Schutzer, Col. 1, Par. 0010, lines 9-10). Brainard discloses authentication code 490A being created at authentication device 420 based on the stored secret (K) and the password (P) (Brainard, Fig. 3). Therefore, it is obvious to create an authentication code at authentication device 420 for another device based on the stored secret (K) and the password (P) as described by Schutzer and Brainard if desired].

Regarding claim 34, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 32, wherein the means for creating involves a bijective locking function, the input parameters of which include the token secret and a one-way function of the password**" as [Brianard discloses that an authentication code may be generated by encrypting the hash value of the password

and/or other values using the stored secret as an encryption key (Brainard, Col. 10, lines 58-61, Col. 14, lines 65-67, and Col. 15, lines 1-2)].

Regarding claim 37, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25, further comprising means for sending an authentication response message from the second unit**" as [Brainard discloses a message may be communicated to the user 410 (first unit) from computer 440 (second unit) to indicate whether the authentication was successful (Brainard, Fig. 3, Col. 16, lines 24-26)].

Regarding claim 39, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25, wherein policies defining critical operations for which authentication is needed"** as [By disclosing critical operations such as paying funds, moving money and the like require a user to authenticate himself or herself (Schutzer, Col. 4, Par. 0032, lines 1-3), Schutzer makes it obvious that critical operations for which authentication is needed are listed in policies of the financial institution's system. Therefore, it is obvious to list critical operations which need user authentication in policies of at least one of the devices if desired].

Regarding claim 41, Brainard discloses "**A first device belonging to a group of at least two devices associated with a common password, and including means for password-based authentication**" as [user 110 and authentication device

120 (corresponding to user 410 and authentication device 420 in Fig. 3) (first device) and verification computer 150 and computer 140 (corresponding to verification computer 450 and computer 440 in Fig. 3) (second device) share a secret PIN or password (Fig. 1, Col. 10, lines 50-52 and Col. 5, line 17). Therefore, user 410 and authentication device 420 (first device) and verification computer 450 and computer 440 (second device) share a secret PIN or password] "**the first device comprises: means for receiving a password**;" as [authentication device 420 allows a user 410 to enter a PIN using a user input interface 412 (keypad) (Col. 14, lines 12-14)] "**based on the password such that each authentication token is irreversibly determined by the password**;" as [the PIN (P) can be mapped to another value with a one-way (irreversible) function before being provided as an input to the combination function to generate an authentication code (Col. 10, lines 58-61)] "**means for determining a check token for a second device in the group based on the password**" as [authentication code 490A for computer 440 and verification computer 450 (second device) is generated based on the password or PIN (P1) at authentication device 420 (first device) (Fig. 3)] "**and means for transmitting the check token to the second device for authentication towards the second device**" as [authentication code 490A is transmitted to computer 440 and verification computer 450 (second device) and is compared with authentication code 490B (Fig. 3, Col. 15, lines 28-29 and Col. 16, lines 9-10)] "**wherein the means for determining the check token further comprises: means for creating the check token for the second device based on the token secret and the password**" as [Brainard discloses authentication code 490A is created

at authentication device 420 based on the stored secret and the password (Brainard, Fig. 3) and is transmitted to computer 440 (Brainard, Col. 15, lines 28-29]

Although Brainard discloses generating authentication tokens based on the password such that each authentication token is irreversibly determined by the password, Brainard does not specifically disclose **means for assigning individual authentication tokens to other devices in the group.** Although Brainard discloses means for determining, at a first device, a check token for a second device based on the password, Brainard does not specifically disclose **means for determining a check token for a second device in the group based on the authentication token of the first device.** In addition, Brainard does not specifically disclose **means for retrieving the token secret using the authentication token of the first device and the password.**

However, Schutzer discloses assigning individual authentication tokens to respective units in a group based on a password such that each authentication token is irreversibly determined by the password (Par. 0010, lines 8-9 and pars. 0010 or 0024-0025).

Schutzer and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Brainard's authentication method by means for assigning individual authentication tokens to other devices in the group as described by Schutzer

since it would provide for the purpose of strong but convenient authentication (Schutzer, Col. 1, Par. 0002, line 3).

Furthermore, Kaufman discloses determining, at a first unit (i.e. workstation), a check token (i.e. transmission code) for a second unit (i.e. server) based on an authentication token (i.e. token) of the first unit (col. 9, lines 41-44 and col. 10, lines 18-20). In addition, Kaufman discloses determining, at a first unit (i.e. workstation), a token secret (i.e. password | token or hash (password | token)) using the authentication token of the first unit (i.e. token) and the password (i.e. password) in generating the check token (col. 9, line 62 - col. 10, line 5).

Kaufman, Schutzer, and Brainard are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer by including means for determining a check token for a second device in the group based on the authentication token of the first device and means for retrieving the token secret using the authentication token of the first device and the password as described by Kaufman for the purpose of obtaining an improved method by which a user or other principal in a computing system may authentication to a computer system (Kaufman, col. 1, lines 13-19).

Regarding claim 45, Brainard in view of Schutzer and further in view of Kaufman discloses "**The device of claim 41, wherein the means for assigning**

further comprises: means for determining a token secret common for the group and non-correlated with the password" as [a stored secret (K) which is non-correlated with the password or PIN (P) is determined at authentication device 120 (corresponding to authentication device 420 shown in Fig. 3) (Brainard, Col. 8, lines 51-53). Therefore, a stored secret (K) is also determined at authentication device 420. Furthermore, this stored secret (K) is accessible to both the authentication device 120 and the verification computer 150 (corresponding to verification computer 450 shown in Fig. 3) (Brainard, Col. 8, lines 60-63). Hence, the stored secret (K) is accessible to both the authentication device 420 (first unit) and verification computer 450 (second unit)] "**and means for creating the authentication token for another device in the group based on the token secret and the password**" as [Schutzer discloses an authentication code being assigned to a user (Schutzer, Col. 1, Par. 0010, lines 9-10). Brainard discloses authentication code 490A being created at authentication device 420 based on the stored secret (K) and the password (P) (Brainard, Fig. 3). Therefore, it is obvious to create an authentication code at authentication device 420 for another device based on the stored secret (K) and the password (P) as described by Schutzer and Brainard if desired].

8. **Claims 2**, **26**, and **42** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman and further in view of Uskela US 6,721,886 (hereinafter "Uskela").

Regarding claim 2, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1**," but does not specifically disclose "**further comprising the step of: deleting the password and all significant parameters generated in the authentication procedure except the authentication tokens after usage thereof**."

However, Uskela discloses a method for preventing unauthorized use of services wherein authentication, verification, and user data generated during authentication are deleted from memory after authentication (Col. 5, lines 40-43).

Uskela, Brianard, Schutzer and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the time of the invention to modify the authentication method of Brainard in view of Schutzer and further in view of Kaufman by deleting sensitive data such as user data (password), authentication and verification data (intermediate parameters) generated during authentication after usage except provided authentication tokens as described by Uskela since it would provide a safety measure against the security risk pointed out by Uskela (Uskela, Col. 5, lines 39-40).

Regarding claim 26, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," but does not specifically disclose "**further comprising: means for deleting the password and parameters generated**

in the authentication procedure except the authentication tokens after usage thereof."

However, Uskela discloses a system for preventing unauthorized use of services wherein authentication, verification, and user data generated during authentication are deleted from memory after authentication (Col. 5, lines 40-43).

Uskela, Brianard, Schutzer and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the time of the invention to modify the authentication system of Brainard in view of Schutzer and further in view of Kaufman by deleting sensitive data such as user data (password), authentication and verification data (intermediate parameters) generated during authentication after usage except provided authentication tokens as described by Uskela since it would provide a safety measure against the security risk pointed out by Uskela (Uskela, Col. 5, lines 39-40).

Regarding claim 42, Brainard in view of Schutzer and further in view of Kaufman discloses "**The device of claim 41**," but does not specifically disclose "**further comprising means for deleting the password and parameters generated in the authentication procedure except the authentication token after usage thereof**."

However, Uskela discloses a system for preventing unauthorized use of services wherein authentication, verification, and user data generated during authentication are deleted from memory after authentication (Col. 5, lines 40-43).

Uskela, Brianard, Schutzer and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the time of the invention to modify the authentication system of Brainard in view of Schutzer and further in view of Kaufman by deleting sensitive data such as user data (password), authentication and verification data (intermediate parameters) generated during authentication after usage except provided authentication tokens as described by Uskela since it would provide a safety measure against the security risk pointed out by Uskela (Uskela, Col. 5, lines 39-40).

9. **Claims 3, 5, 6, 27, 29-30 and 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser et al. US 5,778,065 (hereinafter "Hauser").

Regarding claim 3, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1**," but does not specifically disclose "**further comprising the step of: accepting, at the second unit in response to a successful authentication, update information securely transferred from the first unit, at least a portion of the update information being created at the first unit**."

However, Hauser discloses an authentication server in response to a successful authentication, accepting update information (new key or password) securely transferred (encrypted under present key) from a user and the update information is created by the user (Col. 2, lines 31-32, 34-36, and 44).

Hauser, Brianard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer and further in view of Kaufman by having the second unit accepting update information securely transferred from the first unit in response to a successful authentication as described by Hauser for security reasons since passwords or keys are necessary to communicate safely between users or between users and servers (Hauser, Col.1, lines 13 and 22-24).

Regarding claim 5, Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser discloses "**The method of claim 3, wherein the update information relates to a password change**" as [Hauser discloses a user requesting a password change or update with an authentication server (Hauser, Col. 7, lines 10-11)].

Regarding claim 6, Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser discloses "**The method of claim 3, wherein the update**

information is selected from the group of: new authentication tokens, a new group key, a group-defining list, and, a revocation list, including combinations thereof" as [Hauser discloses a user requesting key update (Knew) which is to be shared between user and authentication server (Hauser, Col. 7, lines 10-11 and Col. 3, line 33)].

Regarding claim 27, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," but does not specifically disclose "**further comprising: means for transferring update information from the first unit to the second unit; and, means for accepting, at the second unit, update information from the first unit in response to a successful authentication**."

However, Hauser discloses an authentication server in response to a successful authentication, accepting update information (new key or password) securely transferred (encrypted under present key) from a user and the update information is created by the user (Col. 2, lines 31-32, 34-36, and 44).

Hauser, Brianard, Schutzer and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer and further in view of Kaufman by having the second unit accepting update information securely transferred from the first unit in response to a successful authentication as described by Hauser for security reasons since passwords or keys are necessary to

communicate safely between users or between users and servers (Hauser, Col.1, lines 13 and 22-24).

Regarding claim 29, Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser discloses "**The system of claim 27, wherein the update information relates to a password change**" as [Hauser discloses a user requesting a password change or update with an authentication server (Hauser, Col. 7, lines 10-11).]

Regarding claim 30, Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser discloses "**The system of claim 27, wherein the update information is selected from the group of: new authentication tokens, a new group key, a group-defining list, and a revocation list, including combinations thereof**" as [Hauser discloses a user requesting key update (Knew) which is to be shared between user and authentication server (Hauser, Col. 7, lines 10-11 and Col. 3, line 33)].

Regarding claim 43, Brainard in view of Schutzer and further in view of Kaufman discloses "**The device of claim 41**," but does not specifically disclose "**further comprising: means for creating update information for the second device; and, means for securely transferring update information to the second device**."

However, Hauser discloses a user creating update information (new key or password) for an authentication server and securely transferred (encrypted under present key) update information to the authentication server (Col. 2, lines 31-32, 34-36, and 44).

Hauser, Brianard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Brainard in view of Schutzer and further in view of Kaufman by creating update information and securely transferred the update information as described by Hauser for security reasons since passwords or keys are necessary to communicate safely between users or between users and servers (Hauser, Col.1, lines 13 and 22-24).

10. **Claims 4 and 28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser and further in view of Aiello et al. US 6,397,329 (hereinafter “Aiello”).

Regarding claim **4**, Brianard in view of Schutzer, further in view of Kaufman, and further in view of Hauser discloses "**The method of claim 3**,” but does not specifically disclose “**wherein the update information is associated with revocation of a non-trusted group member**.”

However, Aiello disclose a certificate authority (CA) periodically generates and signs a complete certificate revocation list (CRL) or a modification of a previous list or revoked certificates (Col. 4, lines 13-16).

Aiello, Brainard, Schutzer, Kaufman and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser by having the update information associating with revocation of a non-trusted group members as described by Aiello since it would provide for the purpose of verifying the authenticity of a presented identity (Aiello, Col. 6, lines 23-24).

Regarding claim 28, Brianard in view of Schutzer, further in view of Kaufman and further in view of Hauser discloses "**The system of claim 27**," but does not specifically disclose "**wherein the update information is associated with revocation of a non-trusted group member**."

However, Aiello disclose a certificate authority (CA) periodically generates and signs a complete certificate revocation list (CRL) or a modification of a previous list or revoked certificates (Col. 4, lines 13-16).

Aiello, Brainard, Schutzer, Kaufman, and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication system of Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser by having the update information associating with revocation of a non-trusted group members as described by Aiello since it would provide for the purpose of verifying the authenticity of a presented identity (Aiello, Col. 6, lines 23-24).

11. **Claims 7-8, 31 and 44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser, and further in view of Matsumoto US 6,215,877 (hereinafter "Matsumoto").

Regarding claim 7, Brainard in view of Schutzer, further in view of Kaufman, and further in view of Hauser discloses "**The method of claim 3**," but does not specifically disclose "**further comprising the step of delegating update rights to a third intermediate unit, and sending at least a portion of the update information for the second unit to the intermediate unit**."

However, Matsumoto disclose a key management server generates a new channel secret key for a chat client, delegates update rights (right to transmit the new key to the chat client) to a chat server and transmits this newly generated channel secret key to the chat server to be sent to a chat client (Fig. 6, Col. 1, lines 61-64 and Col. 10, lines 45-49).

Matsumoto, Brainard, Schutzer, Kaufman and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the authentication method of Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser by delegating update rights to a third intermediate unit as described by Matsumoto since it would provide for the purpose of preventing eavesdropping (Matsumoto, Col. 1, lines 42-44).

Regarding claim 8, Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser, and further in view of Matsumoto discloses "**The method of claim 7, wherein the update information is accompanied by a time stamp for determining whether the update information is still valid when the intermediate unit encounters the second unit**" as [Matsumoto discloses the deadline of the key is written in the channel secret key for determining the validity of the channel secret key (Matsumoto, Col. 10, lines 45-49). In addition, Hauser also discloses including freshness information in update information to determine its validity (Hauser, Col. 2, lines 33 and 43-44)].

Regarding claim 31, Brainard in view of Schutzer, further in view of Kaufman, and further in view of Hauser discloses "**The system of claim 27**," but does not specifically disclose "**further comprising means for delegation of update rights to a**

third intermediate unit, and means for sending at least a portion of the update information for the second unit to the intermediate unit."

However, Matsumoto disclose a key management server generates a new channel secret key for a chat client, delegates update rights (right to transmit the new key to the chat client) to a chat server and transmits this newly generated channel secret key to the chat server to be sent to a chat client (Fig. 6, Col. 1, lines 61-64 and Col. 10, lines 45-49).

Matsumoto, Brainard, Schutzer, Kaufman, and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the authentication system of Brainard in view of Schutzer, further in view of Kaufman, and further in view of Hauser by delegating update rights to a third intermediate unit as described by Matsumoto since it would provide for the purpose of preventing eavesdropping (Matsumoto, Col. 1, lines 42-44).

Regarding claim 44, Brainard in view of Schutzer, further in view of Kaufman, and further in view of Hauser does not specifically disclose "**further comprising means for delegation of update rights to an intermediate device, and means for sending update information for the second device to the intermediate device**."

However, Matsumoto disclose a key management server generates a new channel secret key for a chat client, delegates update rights (right to transmit the new key to the chat client) to a chat server and transmits this newly generated channel

secret key to the chat server to be sent to a chat client (Fig. 6, Col. 1, lines 61-64 and Col. 10, lines 45-49).

Matsumoto, Brainard, Schutzer, Kaufman and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the authentication system of Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser by delegating update rights to a third intermediate unit as described by Matsumoto since it would provide for the purpose of preventing eavesdropping (Matsumoto, Col. 1, lines 42-44).

12. **Claim 9** is rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser, further in view of Matsumoto, and further in view of Gunter et al. US 6,885,388 (hereinafter "Gunter").

Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser and further in view of Matsumoto discloses "**The method of claim 7**," but does not specifically disclose "**wherein the delegation of update rights comprises delegation of rights to further delegate update rights**."

However, Gunter discloses delegation of permission comprises the authority to delegate one or more further permissions to subsequent delegates (Col. 2, lines 40-41).

Gunter, Brainard, Schutzer, Kaufman, Hauser, and Matsumoto are analogous art because they are in the same field of endeavor of data security.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the authentication method of Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser and further in view of Matsumoto by having delegation of update rights comprises delegation of rights to further delegate as described by Gunter since it would provide for the purpose of secure and convenient distribution of sensitive content and services (Gunter, Col. 2, lines 23-24).

13. **Claims 16-17, 23, 35-36, and 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman, and further in view of Jackson et al. US 4,980,542 (hereinafter "Jackson").

Regarding claim 16, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1**," but does not specifically disclose "**wherein implementing policies in at least one of the units in the group for limiting the number and/or frequency of authentication attempts**."

However, Jackson discloses implementing policies for limiting the number of authentication attempts in a smart card's header section (Col. 6, lines 10-11, lines 30-31, and lines 32-38).

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer and further in view of Kaufman by implementing policies for limiting the number of

authentication attempts as described by Jackson since it would provide a convenient yet secure system (Jackson, Col. 2, lines 20-21).

Regarding claim 17, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1**," but does not specifically disclose "**further comprising the step of generating an alarm signal if the number of authentication attempts exceeds a predetermined value**."

However, Jackson discloses a user card sending a PIN error message to a terminal if no valid PIN has been entered after three attempts (Col. 11, lines 37-42).

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer and further in view of Kaufman by generating an alarm message if the number of authentication attempts exceeds a predetermined value as described by Jackson since it would provide a convenient yet secure system (Jackson, Col. 2, lines 20-21).

Regarding claim 23, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1**," but does not specifically disclose "**wherein the group of units constitutes a Personal Area Network (PAN)**."

However, Jackson discloses a postage meter accounting system shown in Fig. 3 which constitutes a Personal Area Network.

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer and further in view of Kaufman by implementing this authentication method in a personal area network (PAN) as described by Jackson since it would provide a convenient and secure system (Jackson, Col. 2, lines 20-21).

Regarding claim 35, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," but does not specifically disclose "**wherein policies implemented in at least one of the units in the group for limiting the number and/or frequency of authentication attempts**."

However, Jackson discloses implementing policies for limiting the number of authentication attempts in a smart card's header section (Col. 6, lines 10-11, lines 30-31, and lines 32-38).

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication system of Brainard in view of Schutzer and further in view of Kaufman by implementing policies for limiting the number of authentication attempts as described by Jackson since it would provide a convenient yet secure system (Jackson, Col. 2, lines 20-21).

Regarding claim 36, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," but does not specifically disclose "**further comprising means for generating an alarm signal if the number of authentication attempts exceeds a predetermined value**."

However, Jackson discloses a user card sending a PIN error message to a terminal if no valid PIN has been entered after three attempts (Col. 11, lines 37-42).

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication system of Brainard in view of Schutzer and further in view of Kaufman by generating an alarm message if the number of authentication attempts exceeds a predetermined value as described by Jackson since it would provide a convenient yet secure system (Jackson, Col. 2, lines 20-21).

Regarding claim 40, Brainard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," but does not specifically disclose "**wherein said communication system being a Personal Area Network (PAN)**."

However, Jackson discloses a postage meter accounting system shown in Fig. 3 which constitutes a Personal Area Network.

Jackson, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication system of Brainard in view of Schutzer and further in view of Kaufman by implementing this authentication system in a personal area network (PAN) as described by Jackson since it would provide a convenient and secure system (Jackson, Col. 2, lines 20-21).

14. **Claims 19-20**, **24, and 38** are rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman and further in view of MacKenzie US 7,076,656 (hereinafter "MacKenzie").

Regarding claim 19, Brianard in view of Schutzer disclose "**The method of claim 1**," but does not specifically disclose "**further comprising the step of authentication of the second unit towards the first unit, whereby the first and second units are mutually authenticated towards each other**."

However, MacKenzie discloses mutual authentication between two parties A and B (Col. 8, lines 64-65).

MacKenzie, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer and further in view of Kaufman by including mutual authentication between two devices as described by MacKenzie since it would provide security against attacks by adversaries (MacKenzie, Col. 4, lines 19-21).

Regarding claim 20, Brainard in view of Schutzer, further in view of Kaufman, and further in view of MacKenzie discloses "**The method of claim 19, further comprising the steps of: generating a respective random value at the first and second unit; determining temporary test secrets at the first and second unit based on the random values; and, exchanging the temporary test secrets between the first and second unit for mutual authentication purposes**" as [MacKenzie discloses A generating random x and B generating random y; determining test secrets k and k'; and exchanging test secrets between A and B for mutual authentication (MacKenzie, Fig. 3)].

Regarding claim 24, Brainard in view of Schutzer and further in view of Kaufman discloses "**The method of claim 1,**" but does not specifically disclose **"wherein the authentication tokens are tamper-resistantly stored in the respective units**."

However, MacKenzie discloses persistent stored data being tamper-proof (Col. 2, lines 22-26).

MacKenzie, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication method of Brainard in view of Schutzer and further in view of Kaufman by tamper-proofing stored authentication codes (persistent

stored data) in respective devices as described by MacKenzie since it would provide extra security against attack by adversaries (MacKenzie, Col. 2, lines 27-29).

Regarding claim 38, Brianard in view of Schutzer and further in view of Kaufman discloses "**The system of claim 25**," as but does not specifically disclose "**further comprising means for mutual authentication between two units in the group**."

However, MacKenzie discloses mutual authentication between two parties A and B (Col. 8, lines 64-65).

MacKenzie, Brainard, Schutzer, and Kaufman are analogous art because they are in the same field of endeavor of authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify authentication system of Brainard in view of Schutzer and further in view of Kaufman by including mutual authentication between two devices as described by MacKenzie since it would provide security against attacks by adversaries (MacKenzie, Col. 4, lines 19-21).

15. **Claim 22** is rejected under 35 U.S.C. 103(a) as being unpatentable over Brainard in view of Schutzer, further in view of Kaufman, further in view of Hauser, and further in view of McDowell et al. US 6,668,167 (hereinafter "McDowell").

Brianard in view of Schutzer, further in view of Kaufman, and further in view of Hauser discloses "**The method of claim 3,**" but does not specifically disclose

"wherein a unit that is switched-on after being inactive for a predetermined period of time automatically requests appropriate update information from at least two other units."

However, McDowell discloses a MS that is turned on after being inactive for a predetermined period of time automatically requests update information (new TMSI) from the MSC and VLR (Fig. 14, Col. 10, lines 54-55).

McDowell, Brainard, Schutzer, Kaufman and Hauser are analogous art because they are in the same field of endeavor of data security and authentication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the authentication method of Brainard in view of Schutzer, further in view of Kaufman and further in view of Hauser by having a unit after switched-on automatically requests update information as described by McDowell since it would provide for the purpose of receiving important update information (McDowell, Col. 10, lines 54-55).

Conclusion

Applicants' amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/T. N/
Examiner